# THE AVERAGE LEAST CHARACTER NONRESIDUE AND FURTHER VARIATIONS ON A THEME OF ERDŐS

GREG MARTIN AND PAUL POLLACK

Abstract. For each nonprincipal Dirichlet character $\chi$, let $n_\chi$ be the least $n$ with $\chi(n) \notin \{0,1\}$. For each prime $p$, let $\chi_p(\cdot) = \left(\frac{\cdot}{p}\right)$ be the quadratic character modulo $p$. In 1961, Erdős showed that $n_{\chi_p}$ possesses a finite mean value as $p$ runs over the odd primes in increasing order. We show that as $q \to \infty$, the average of $n_\chi$ over *all* nonprincipal characters $\chi$ modulo $q$ is $\ell(q) + o(1)$, where $\ell(q)$ denotes the least prime not dividing $q$. Moreover, if one averages over all nonprincipal characters of moduli $\le x$, the average approaches (as $x \to \infty$) the limiting value

$$\sum_{\ell} \frac{\ell^2}{\prod_{p \le \ell}(p+1)} \approx 2.5350541804,$$

where the sum is over primes $\ell$ and the product is over primes $p \le \ell$.

One can also view Erdős's theorem as giving the average size of the least non-split prime in the quadratic field of conductor $p$, where again $p$ runs over odd primes. Similar results with the average taken over all quadratic fields were recently proved by the second author. In this paper, we prove a result of this type for cubic number fields: If one averages over all cubic fields $K$, ordered by discriminant, then the mean value of the least rational prime that does not split completely in $K$ is

$$\sum_{r} \frac{r(5/6 + 1/r + 1/r^2)}{1 + 1/r + 1/r^2} \prod_{p<r} \frac{1/6}{1 + 1/p + 1/p^2} \approx 2.1211027269,$$

where the sum is over all primes $r$.

## 1. Introduction

For a nonprincipal Dirichlet character $\chi$, let $n_\chi$ denote the least character nonresidue for $\chi$, that is, the least positive integer $n$ with $\chi(n) \neq 0$ and $\chi(n) \neq 1$. Under the assumption of the generalized Riemann hypothesis for Dirichlet $L$-functions, we know that $n_\chi \le 3 \log^2 q$ for every nonprincipal character $\chi$ (mod $q$). (As stated this result is due to Bach [Bac90, Theorem 3], although the first result of its kind was proved by Ankeny [Ank52]. If $q$ is prime, then $\chi$ is a $k$th power residue character for some $k$ dividing $q-1$, and the study of the maximal order of $n_\chi$ goes back to Vinogradov and Linnik in the early part of the twentieth century.) The best unconditional result in this direction, due to Norton (see [Nor98, equation (1.22)]), asserts that $n_\chi \ll_\epsilon q^{1/4\sqrt{e}+\epsilon}$ for every nonprincipal character $\chi$ (mod $q$).

Short of a satisfactory unconditional "pointwise" result, one can study $n_\chi$ on average. Erdős [Erd61] was the first to adopt this viewpoint in his treatment of quadratic characters $\chi(\cdot) = \left(\frac{\cdot}{p}\right)$ modulo primes $p$. He showed that

$$\lim_{x\to\infty} \left( \pi(x)^{-1} \sum_{2<p\le x} n_{\left(\frac{\cdot}{p}\right)} \right) = \sum_{k=1}^{\infty} \frac{p_k}{2^k}, \tag{1.1}$$

where $p_k$ denotes the $k$th prime in increasing order. In other words, the average value of the least quadratic nonresidue modulo a prime is the constant $\sum_{k=1}^{\infty} p_k/2^k \approx 3.67464$.

2010 *Mathematics Subject Classification.* Primary 11A15, Secondary 11L40, 11R16.

This result was extended to all real primitive characters by the second author [Pol11], who showed that

$$\lim_{x\to\infty}\bigg(\sum_{|D|\le x} 1\bigg)^{-1}\bigg(\sum_{|D|\le x} n_{(\frac{D}{\cdot})}\bigg) = \sum_{\ell} \frac{\ell^2}{2(\ell+1)} \prod_{p<\ell} \frac{p+2}{2(p+1)}, \tag{1.2}$$

where the sums on the left-hand side are over fundamental discriminants $D$ whose absolute value is at most $x$, and the sum and product on the right-hand side are over primes $\ell$ and $p$. In other words, the average least character nonresidue of a general quadratic character is the constant on the right-hand side of equation (1.2), which is approximately 4.98085.

Our first goal in this paper is to understand the average of $n_\chi$ taken over *all* nonprincipal characters $\chi$. Let $\ell(q)$ denote the least prime not dividing $q$. If $\chi$ is any character modulo $q$, then $\chi(n) = 0$ whenever $1 < n < \ell(q)$; hence $n_\chi \ge \ell(q)$ for all nonprincipal characters $\chi$. We prove that the average of $n_\chi$ over all nonprincipal characters modulo $q$ is always very close to $\ell(q)$:

**Theorem 1.1.** *For $q \ge 3$, we have*

$$\frac{1}{\phi(q)-1} \sum_{\substack{\chi \ (\mathrm{mod}\ q)\\ \chi\ne\chi_0}} n_\chi = \ell(q) + O\bigg(\frac{(\log\log q)^3}{\log q}\bigg).$$

One consequence of Theorem 1.1 is an analogue of the average value results (1.1) and (1.2), but with the average taken over all nonprincipal characters with conductor at most $x$:

**Corollary 1.2.** *Define*

$$\Delta = \sum_{\ell} \frac{\ell^2}{\prod_{p\le\ell}(p+1)} \approx 2.5350541804, \tag{1.3}$$

*where the sum and product are taken over primes $\ell$ and $p$. Then*

$$\lim_{x\to\infty}\bigg(\sum_{q\le x} \sum_{\substack{\chi \ (\mathrm{mod}\ q)\\ \chi\ne\chi_0}} 1\bigg)^{-1}\bigg(\sum_{q\le x} \sum_{\substack{\chi \ (\mathrm{mod}\ q)\\ \chi\ne\chi_0}} n_\chi\bigg) = \Delta.$$

We remark that our methods can also address the analogues of Theorem 1.1 and Corollary 1.2 in which the sums over characters $\chi$ are restricted to primitive characters only (see equation (3.4) and Theorem 3.6).

One can also view (1.1) and (1.2) as results in algebraic number theory. If $\chi$ is the quadratic character modulo $p$, then $n_\chi$ is the least prime that does not split in the quadratic field of conductor $p$ (equivalently, of discriminant $(-1)^{(p-1)/2}p$). Thus, Erdős's theorem gives the average least non-split prime in a quadratic extension, where the average is restricted to quadratic fields of prime conductor. Similarly, (1.2) is an estimate for the average least inert prime, where now the average is taken over all quadratic fields, ordered by discriminant.

For a prime $p \equiv 1 \pmod 3$, define $n_3(p)$ as the least cubic nonresidue modulo $p$. Elliott [Ell68] showed that $n_3(p)$ possesses a finite mean-value. (In fact, he showed the analogous result for $k$th power nonresidues, for all $k$.) We can interpret Elliott's result on $n_3(p)$ as the determination of the average least non-split prime, with the average restricted to cyclic cubic extensions of prime conductor. Our second theorem gives the average least non-split prime, with the average taken over *all* cubic extensions of

$\mathbb{Q}$, ordered by discriminant. In what follows, we write $D_K$ for the discriminant of the number field $K$.

**Theorem 1.3.** *For a cubic number field $K$, let $n_K$ denote the least rational prime that does not split completely in $K$. Define*

$$\Delta_{nsc} = \sum_{\ell} \frac{5\ell^3+6\ell^2+6\ell}{6(\ell^2+\ell+1)} \prod_{p<\ell} \frac{p^2}{6(p^2+p+1)} \approx 2.1211027269, \tag{1.4}$$

*where the sum and product are taken over primes $\ell$ and $p$. Then*

$$\lim_{x\to\infty} \bigg( \sum_{|D_K|\le x} 1 \bigg)^{-1} \bigg( \sum_{|D_K|\le x} n_K \bigg) = \Delta_{nsc},$$

*where the sums on the left-hand side are taken over (all isomorphism classes of) cubic fields $K$ for which $|D_K| \le x$.*

**Remark.** As a reality check, we sampled cubic fields with discriminant near $-10^{12}$. Using K. Belabas's `cubics` package (see [Bel97, Bel04]) and `PARI/GP`, we found that the average of $n_K$ over cubic fields $K$ with $|D_K + 10^{12}| \le 250{,}000$ is about 2.12065, a close match to the limiting constant $\Delta_{nsc}$.

The subscript of $\Delta_{nsc}$, which stands for "not split completely", suggests that one can also calculate the average value of the least prime with other behaviors (split completely, or partially split, or inert) in cubic extensions of $\mathbb{Q}$. We can indeed establish these additional average values (see Theorem 4.8), but only under the assumption of a generalized Riemann hypothesis.

The proofs of our theorems, while similar in flavor to the arguments of [Erd61, Pol11], employ different tools. For the proof of Theorem 1.1, our primary inspiration was a paper of Burthe [Bur97], which uses zero-density estimates and a theorem of Montgomery (Proposition 2.1 below) to prove that

$$\frac{1}{x} \sum_{q\le x} \max_{\substack{\chi \pmod q \\ \chi\ne\chi_0}} n_\chi \ll (\log x)^{97};$$

note that Burthe's result shows unconditionally that a bound of the same flavor as Bach's $n_\chi \le 3\log^2 q$ holds on average. The proof of Theorem 1.3 involves a few different ingredients; perhaps most crucial is the recent work of Taniguchi and Thorne [TT11] on counting cubic fields with prescribed local conditions (see Proposition 4.2).

**Notation.** The letters $\ell$, $p$, and $r$ are reserved for prime variables. We write $P(n)$ for the largest prime factor of $n$ and $\ell(n)$ for the smallest prime *not* dividing $n$. We say that $n$ is *$y$-friable* (or *$y$-smooth*) if $P(n) \le y$, and we let $\Psi(x,y)$ denote the number of $y$-friable integers not exceeding $x$. We write $\omega(n) = \sum_{p|n} 1$ for the number of distinct prime factors of $n$ and $\Omega(n) = \sum_{p^k|n} 1$ for the number of prime factors of $n$ counted with multiplicity. We use $c_1, c_2, \dots$ for absolute positive constants.

## 2. The average least character nonresidue (mod $q$)

We begin by quoting two theorems from the literature. The first, due to Montgomery [Mon94, Theorem 1, p. 164] (compare with [LMO79]), relates the size of $n_\chi$ to a zero-free region for $L(s,\chi)$ near $s=1$. Define $N(\sigma,T,\chi)$ as the number of zeros $s=\beta+i\gamma$ of $L(s,\chi)$ with $\sigma\le\beta\le 1$ and $|\gamma|\le T$.

**Proposition 2.1.** *Let $\chi$ be a nonprincipal Dirichlet character modulo $q$, and let $\delta$ be a real number in the range $1/\log q < \delta \le \frac{1}{2}$. If $N(1-\delta, \delta^2 \log q, \chi) = 0$, then $n_\chi < (c_1 \delta \log q)^{1/\delta}$. Here $c_1 > 0$ is an absolute constant.*

The second, due to Jutila [Jut77, Theorem 1]), is a zero-density estimate for the collection of characters to a given modulus.

**Proposition 2.2.** *Let $\epsilon > 0$. For $4/5 \le \alpha \le 1$ and $T \ge 1$, we have*

$$\sum_{\chi \pmod q} N(\alpha, T, \chi) \ll_\epsilon (qT)^{(2+\epsilon)(1-\alpha)}.$$

These propositions allow us to establish the next lemma, which will eventually be used to show that characters $\chi$ with $n_\chi$ larger than about $(\log q)^5$ do not significantly affect the average of $n_\chi$.

**Lemma 2.3.** *There exists an absolute constant $c_2 > 0$ such that for any positive integer $q$, the number of characters $\chi \pmod q$ with $n_\chi \ge c_2 \log^5 q$ is $\ll q^{0.43}$.*

*Proof.* We may assume that $q \ge e^{25}$, and we set $c_2 = (\frac{c_1}{5})^5$ where $c_1$ is the constant from Proposition 2.1. That proposition with $\delta = \frac{1}{5}$ implies that the number of nonprincipal $\chi$ with $n_\chi \ge (\frac{c_1}{5} \log q)^5 = c_2 \log^5 q$ is bounded above by

$$\#\biggl\{\chi \pmod q \colon N\biggl(\frac{4}{5}, \frac{\log q}{25}, \chi\biggr) \ge 1\biggr\} \le \sum_{\chi \pmod q} N\biggl(\frac{4}{5}, \frac{\log q}{25}, \chi\biggr).$$

From Proposition 2.2 with $\alpha = \frac{4}{5}$ and $\epsilon = \frac{1}{10}$, this sum is $\ll (q \log q)^{21/50} \ll q^{0.43}$. □

We also need an elementary lemma concerning the structure of the character group.

**Lemma 2.4.** *Let $G$ be a finite abelian group and $H \le G$ a subgroup. The number of homomorphisms $\chi \colon G \to \mathbb{C}^\times$ such that $\chi(h) = 1$ for all $h \in H$ is exactly $\#G/\#H$. In particular, if $H$ is a subgroup of the multiplicative group $(\mathbb{Z}/q\mathbb{Z})^\times$, then the number of Dirichlet characters $\chi \pmod q$ such that $\chi(h) = 1$ for all $h \in H$ is exactly $\phi(q)/\#H$.*

The proof of Lemma 2.4 is simple; the homomorphisms $\chi \colon G \to \mathbb{C}^\times$ that are trivial on $H$ are in canonical bijection with the homomorphisms $\tilde{\chi} \colon G/H \to \mathbb{C}^\times$, the number of which is $\#G/\#H$ (compare with [Ser73, Chapter VI, §1.1]).

The next lemma reduces the proof of Theorem 1.1 to the task of bounding two expressions in its error term. In addition to the notation $\ell(q)$ for the least prime not dividing $q$, we define $f(q)$ to be the multiplicative order of $\ell(q)$ modulo $q$. We record the helpful estimate $\ell(q) \ll \log q$, which holds because the product of all the primes less than $2 \log q$ (say) is larger than $q$ when $q$ is sufficiently large, by the prime number theorem.

**Lemma 2.5.** *Let $\chi$ be a nonprincipal character $\pmod q$. For any real number $Y$ satisfying $\ell(q) < Y \le c_2 \log^5 q$ (where $c_2$ is the constant from Lemma 2.3), we have*

$$\frac{1}{\phi(q)-1} \sum_{\substack{\chi \pmod q \\ \chi \ne \chi_0}} n_\chi = \ell(q) + O\biggl(\frac{1}{\phi(q)} \sum_{\substack{\chi \pmod q \\ \chi \ne \chi_0 \\ Y < n_\chi \le c_2 \log^5 q}} n_\chi + \frac{Y}{f(q)} + q^{-1/3}\biggr).$$

*Proof.* We begin by writing

$$\frac{1}{\phi(q)-1}\sum_{\substack{\chi \pmod q\\ \chi\ne\chi_0}} n_\chi = \frac{1}{\phi(q)-1}\sum_{\substack{\chi \pmod q\\ \chi\ne\chi_0\\ n_\chi=\ell(q)}} n_\chi + O\bigg(\frac{1}{\phi(q)}\sum_{\substack{\chi \pmod q\\ \chi\ne\chi_0\\ \ell(q)<n_\chi\le Y}} n_\chi + \frac{1}{\phi(q)}\sum_{\substack{\chi \pmod q\\ \chi\ne\chi_0\\ Y<n_\chi\le c_2\log^5 q}} n_\chi + \frac{1}{\phi(q)}\sum_{\substack{\chi \pmod q\\ \chi\ne\chi_0\\ n_\chi>c_2\log^5 q}} n_\chi\bigg). \tag{2.1}$$

By Lemma 2.4 applied to the subgroup of $(\mathbb{Z}/q\mathbb{Z})^\times$ generated by $\ell(q)$, which has order $f(q)$, the number of characters $\chi \pmod q$ with $\chi(\ell(q)) = 1$ equals $\phi(q)/f(q)$. It follows that

$$\frac{1}{\phi(q)-1}\sum_{\substack{\chi \pmod q\\ \chi\ne\chi_0\\ n_\chi=\ell(q)}} n_\chi = \frac{\phi(q)-\phi(q)/f(q)}{\phi(q)-1}\ell(q) = \ell(q) + O\bigg(\frac{\ell(q)}{f(q)}\bigg) = \ell(q) + O\bigg(\frac{Y}{f(q)}\bigg),$$

while the first error term in equation (2.1) can be bounded by

$$\frac{1}{\phi(q)}\sum_{\substack{\chi \pmod q\\ \chi\ne\chi_0\\ \ell(q)<n_\chi\le Y}} n_\chi \le \frac{1}{\phi(q)}\bigg(\frac{\phi(q)}{f(q)}-1\bigg)Y \ll \frac{Y}{f(q)}.$$

As for the last error term in equation (2.1), we use the fact that $n_\chi \ll q^{1/5}$ (this follows from Norton's result quoted in the introduction, since $\frac{1}{4\sqrt{e}} < \frac{1}{5}$). Using this estimate in conjunction with Lemma 2.3, we have the bound

$$\frac{1}{\phi(q)}\sum_{\substack{\chi \pmod q\\ \chi\ne\chi_0\\ n_\chi>c_2\log^5 q}} n_\chi \ll \frac{1}{\phi(q)}q^{0.43}\cdot q^{1/5} \ll q^{-1/3}$$

(here we have used $\phi(q) \gg q/\log\log q \gg q^{0.99}$). The lemma now follows from equation (2.1) and the subsequent estimates. □

Before we proceed, we must quote one more theorem from the literature. This result, due to Baker and Harman [BH96, BH98], asserts that many shifted primes possess a large prime factor.

**Proposition 2.6.** *For each positive real number $\theta \le 0.677$, there is a constant $c_\theta > 0$ with the following property: For $x$ sufficiently large in terms of $\theta$, the number of primes $p \le x$ with $P(p-1) > x^\theta$ is $> c_\theta x/\log x$.*

The following somewhat strange dichotomy will be useful to us in the proof of Theorem 1.1. For the rest of this section, define

$$X = X(q) = \frac{(\log\log q)^3}{\log\log\log q}.$$

**Lemma 2.7.** *If $q$ is a sufficiently large integer, then either $f(q) \gg \exp((\log\log q)^2)$ or there exist at least six primes less than $X$ that do not divide $q$.*

**Remark.** The proof actually yields many more than six small primes: when $f(q)$ is small, we could conclude that there are $\gg X/\log X$ primes less than $X$ that do not divide $q$. We will not need this stronger conclusion, however.

*Proof.* Define $S_0$ to be the set of primes $p \le X$ dividing $q$ and satisfying $P(p-1) > X^{0.67}$. By Proposition 2.6, there are $\gg X/\log X$ primes $p \le X$ with $P(p-1) > X^{0.67}$. Let us assume that there are at most five primes less than $X$ that do not divide $q$ (so that we want to derive the lower bound $f(q) \gg \exp((\log\log q)^2)$); then almost all of these primes obtained from Proposition 2.6 are actually divisors of $q$ (when $q$ is sufficiently large), and so $\#S_0 \gg X/\log X$.

Define $S$ to be the subset of $S_0$ consisting of those primes in $S_0$ having the additional property that the multiplicative order of $\ell(q)$ modulo $p$ is divisible by $P(p-1)$. We claim that $\#S \gg X/\log X$ as well. To see this, note that if $p$ does not have this property, then the order of $\ell(q)$ modulo $p$ is a divisor of $(p-1)/P(p-1)$ and so is less than $X^{0.33}$; hence, $p$ divides an integer of the form $\ell(q)^j - 1$ for some positive integer $j \le X^{0.33}$. On the other hand, each number $\ell(q)^j - 1$ has at most $\log(\ell(q)^j - 1)/\log 2 \ll j \log \ell(q)$ prime factors; furthermore, $\ell(q) \ll \log q$. Therefore the total number of prime factors of all the numbers $\ell(q)^j - 1$ is

$$\ll \sum_{j \le X^{0.33}} j \log \ell(q) \ll X^{0.66} \log\log q \ll X^{0.995}$$

by the definition of $X$. Therefore $\#(S_0 \setminus S) \ll X^{0.995} = o(X/\log X)$, and hence $\#S \gg X/\log X$ as claimed.

If $r$ is a prime exceeding $X^{0.67}$, then the number of $p \in S$ for which $P(p-1) = r$ is clearly bounded by the number of integers in $(1, X]$ that are congruent to $1 \pmod r$, which is at most $X/r < X^{0.33}$. Hence, the number of distinct values of $P(p-1)$, as $p$ ranges over $S$, is $\gg X^{0.67}/\log X$. Since each prime $p$ divides $q$, we know that $f(q)$ is divisible by the order of $\ell(q) \pmod p$ for all $p \in S$, hence divisible by all of these $\gg X^{0.67}/\log X$ distinct primes $P(p-1)$, each of which exceeds $X^{0.67}$. It follows that there exist positive constants $c_3$ and $c_4$ such that

$$\begin{aligned} f(q) \ge (X^{0.67})^{c_3 X^{0.67}/\log X} &\ge \exp(c_4 X^{0.67}) \\ &= \exp\left(\frac{c_4(\log\log q)^{2.01}}{(\log\log\log q)^{0.67}}\right) \gg \exp\left((\log\log q)^2\right) \end{aligned}$$

as desired. □

*Proof of Theorem 1.1.* We may assume that $q$ is sufficiently large. Suppose first that $f(q) \gg \exp((\log\log q)^2)$. Taking $Y = c_2 \log^5 q$ in Lemma 2.5, we see that

$$\frac{1}{\phi(q)-1} \sum_{\substack{\chi \pmod q \\ \chi \ne \chi_0}} n_\chi = \ell(q) + O\biggl(\frac{\log^5 q}{f(q)} + q^{-1/3}\biggr) = \ell(q) + O\biggl(\frac{1}{\exp((\log\log q)^{3/2})}\biggr),$$

say, which is stronger than the error term in the statement of the theorem. By Lemma 2.7, the only case left to consider is the case where there exist at least six primes $p_1, \dots, p_6$ less than $X$ that do not divide $q$.

In particular, $\ell(q) < X$ in this case, so we may take $Y = X$ in Lemma 2.7 to obtain

$$\begin{aligned}\frac{1}{\phi(q)-1} \sum_{\substack{\chi \pmod q \\ \chi \ne \chi_0}} n_\chi &= \ell(q) + O\biggl( \frac{1}{\phi(q)} \sum_{\substack{\chi \pmod q \\ \chi \ne \chi_0 \\ X < n_\chi \le c_2 \log^5 q}} n_\chi + \frac{X}{f(q)} + q^{-1/3} \biggr) \\ &= \ell(q) + O\biggl( \frac{\log^5 q}{\phi(q)} \#\bigl\{ \chi \pmod q \colon n_\chi > X \bigr\} + \frac{X}{f(q)} + q^{-1/3} \biggr).\end{aligned}$$

Since $q \mid (\ell(q)^{f(q)} - 1)$, we have the trivial lower bound $f(q) \ge (\log q)/\log \ell(q)$, and so $X/f(q) \le (X \log \ell(q))/\log q < X \log X/\log q \ll (\log\log q)^3/\log q$. The theorem therefore follows if we can show that

$$\#\bigl\{ \chi \pmod q \colon n_\chi > X \bigr\} \ll \phi(q) \frac{(\log\log q)^3}{(\log q)^6}. \tag{2.2}$$

Let $H$ be the subgroup of $(\mathbb{Z}/q\mathbb{Z})^\times$ generated by (the images of) $p_1, \dots, p_6$. If $n_\chi > X$, then $\chi(h) = 1$ for all $h \in H$; thus by Lemma 2.4,

$$\#\bigl\{ \chi \pmod q \colon n_\chi > X \bigr\} \le \#\bigl\{ \chi \pmod q \colon \chi(h) = 1 \text{ for all } h \in H \bigr\} = \frac{\phi(q)}{\#H}.$$

However, the order of $H$ is at least the number of integers less than $q$ that factor as a product of the $p_i$, which includes every integer of the form $p_1^{\alpha_1} \cdots p_6^{\alpha_6}$ with $0 \le \alpha_1, \dots, \alpha_6 < \log q/(6 \log X)$. Therefore $\#H \ge 6^{-6}((\log q)/\log X)^6$, and so

$$\#\bigl\{ \chi \pmod q \colon n_\chi > X \bigr\} \ll \frac{\phi(q)}{((\log q)/\log X)^6} \ll \phi(q) \frac{(\log\log\log q)^6}{(\log q)^6}.$$

This upper bound is stronger than the required estimate (2.2), which completes the proof of the theorem. □

**Remark.** It is known that $f(q) > q^{1/2}$ for almost all $q$, in the sense of asymptotic density. (This lower bound, and a bit more, follows from [KP05, Theorem 1].) For such $q$, we deduce quickly from Lemma 2.5 that the average of $n_\chi$ is $\ell(q) + O(q^{-1/50})$. Thus, the estimate of Theorem 1.1 is interesting only for integers $q$ for which $f(q)$ is abnormally small. Our proof of Theorem 1.1 can be modified to show that the average of $n_\chi$ is always $\ell(q) + O\bigl(X/f(q) + \exp(-(\log\log q)^2)\bigr)$ in the above notation, and that the term $X/f(q)$ can be omitted when $\ell(q) > X$.

## 3. The least character nonresidue averaged over the modulus $q$

Having established an asymptotic formula for the average of the least character nonresidue $n_\chi$ over all Dirichlet characters $\chi$ to a single modulus, we turn now to averaging $n_\chi$ over all characters with conductor less than $x$. Theorem 1.1 tells us that almost all of the $\phi(q)$ characters modulo $q$ have $n_\chi = \ell(q)$; therefore we should expect the average value of $n_\chi$ over all characters of conductor less than $x$ to be closely related to the sum $\sum_{q \le x} \phi(q)\ell(q)$. This is indeed the case, as the proof of Corollary 1.2 later in this section will show; the majority of the work is in showing how the constant $\Delta$ defined in equation (1.3) arises in connection with that sum (see Proposition 3.5). At the end of this section, we outline how the same methods can be applied to averages over only certain characters; as a concrete example, we establish analogues of Theorem 1.1 and Corollary 1.2 where we average only over primitive characters.

Our first two lemmas establish an asymptotic formula for the summatory function of $\phi(n)$ over integers relatively prime to a fixed number $m$, with enough uniformity in $m$ for our later purposes.

**Lemma 3.1.** *Given a positive integer $m$, let $h(d)$ denote the largest divisor of $d$ that is coprime to $m$. For all $x \ge 3$,*

$$x^2 \sum_{d>x} \frac{\mu^2(d)}{dh(d)} + x \sum_{d \le x} \frac{\mu^2(d)}{h(d)} \ll 2^{\omega(m)} x \log x.$$

*Proof.* We employ Rankin's method. For any real number $0 < \epsilon < 1$, we have

$$\begin{aligned} x^2 \sum_{d>x} \frac{\mu^2(d)}{dh(d)} &+ x \sum_{d \le x} \frac{\mu^2(d)}{h(d)} \\ &< x^2 \sum_{d>x} \frac{\mu^2(d)}{dh(d)} \left(\frac{d}{x}\right)^{1-\epsilon} + x \sum_{d \le x} \frac{\mu^2(d)}{h(d)} \left(\frac{x}{d}\right)^{\epsilon} = x^{1+\epsilon} \sum_{d=1}^{\infty} \frac{\mu^2(d)}{d^\epsilon h(d)}. \end{aligned}$$

The right-hand side can be expressed as the convergent Euler product

$$\begin{aligned} x^{1+\epsilon} \prod_p \left(1 + \frac{1}{p^\epsilon h(p)}\right) &= x^{1+\epsilon} \prod_{p \mid m} \left(1 + \frac{1}{p^\epsilon}\right) \prod_{p \nmid m} \left(1 + \frac{1}{p^{1+\epsilon}}\right) \\ &\le x^{1+\epsilon} 2^{\omega(m)} \prod_p \left(1 + \frac{1}{p^{1+\epsilon}}\right) \\ &= x^{1+\epsilon} 2^{\omega(m)} \frac{\zeta(1+\epsilon)}{\zeta(2+2\epsilon)} \ll 2^{\omega(m)} x^{1+\epsilon} \epsilon^{-1}. \end{aligned}$$

Choosing $\epsilon = 1/\log x$ establishes the required estimate. □

**Lemma 3.2.** *Let $m$ be a natural number. For $x \ge 2$,*

$$\sum_{\substack{n \le x \\ \gcd(n,m)=1}} \phi(n) = \frac{3x^2}{\pi^2} \prod_{p \mid m} \left(1 + \frac{1}{p}\right)^{-1} + O(2^{\omega(m)} x \log x)$$

*uniformly in $m$.*

*Proof.* Let $\chi_0$ be the principal character modulo $m$, and let $h(d)$ denote the largest divisor of $d$ that is coprime to $m$ (as in Lemma 3.1). The identity $\phi(n)\chi_0(n)/n = \sum_{d \mid n} \mu(d)/h(d)$ is easy to verify (since both sides are multiplicative functions, it suffices to check the identity on prime powers); it follows that

$$\begin{aligned} \sum_{\substack{n \le x \\ \gcd(n,m)=1}} \phi(n) &= \sum_{n \le x} n \cdot \frac{\phi(n)\chi_0(n)}{n} = \sum_{n \le x} n \sum_{d \mid n} \frac{\mu(d)}{h(d)} \\ &= \sum_{d \le x} \frac{\mu(d)}{h(d)} \sum_{\substack{n \le x \\ d \mid n}} n = \sum_{d \le x} \frac{\mu(d)}{h(d)} \sum_{e \le x/d} de \\ &= \sum_{d \le x} \frac{\mu(d)}{h(d)} \left(\frac{x^2}{2d} + O(x)\right) = \frac{x^2}{2} \sum_{d \le x} \frac{\mu(d)}{dh(d)} + O\left(x \sum_{d \le x} \frac{\mu^2(d)}{h(d)}\right) \\ &= \frac{x^2}{2} \sum_{d=1}^{\infty} \frac{\mu(d)}{dh(d)} + O\left(x^2 \sum_{d>x} \frac{\mu^2(d)}{dh(d)} + x \sum_{d \le x} \frac{\mu^2(d)}{h(d)}\right). \end{aligned}$$

The error term is $\ll 2^{\omega(m)} x \log x$ by Lemma 3.1, while in the main term, we have

$$\begin{aligned}\sum_{d=1}^{\infty} \frac{\mu(d)}{dh(d)} &= \prod_{p\nmid m}\Big(1-\frac{1}{p^2}\Big)\prod_{p\mid m}\Big(1-\frac{1}{p}\Big)\\ &= \prod_{p}\Big(1-\frac{1}{p^2}\Big)\prod_{p\mid m}\Big(1+\frac{1}{p}\Big)^{-1} = \frac{6}{\pi^2}\prod_{p\mid m}\Big(1+\frac{1}{p}\Big)^{-1}\end{aligned}$$

as claimed. □

Our next goal is to evaluate the sum $\sum_{q\le x}\phi(q)\ell(q)$ that features prominently in the proof of Corollary 1.2. Our method hinges upon sorting these integers $q$ by their largest divisor divisible only by primes not exceeding $2\log x$; the next two lemmas establish some preliminary results concerning sums over these friable numbers.

**Lemma 3.3.** *Let $x \ge 3$, and set $y = 2\log x$.*

(a) $\displaystyle\sum_{\substack{m>x^{1/2}\\ m \text{ is } y\text{-friable}}} \frac{1}{m} \ll x^{-1/3}$*;*

(b) *There are $\ll x^{2/3}$ integers less than $x$ that have a $y$-friable divisor exceeding $x^{1/2}$.*

*Proof.* We may assume that $x$ is sufficiently large. It follows from work of de Bruijn that $\log\Psi(t,y) \ll (\log t)/\log y$ uniformly for $t\ge 2$ and $y \le 4\log t$ (see for example [Ten95, Theorem 2, p. 359]). In particular, with $y = 2\log x$, we have $\Psi(t,y) < t^{1/3}$ uniformly for $t \ge x^{1/2}$, once $x$ is sufficiently large. Hence,

$$\begin{aligned}\sum_{\substack{m>x^{1/2}\\ m \text{ is } y\text{-friable}}} \frac{1}{m} &= \int_{x^{1/2}}^{\infty}\frac{1}{t}\,d\Psi(t,y) = -\frac{\Psi(x^{1/2},y)}{x^{1/2}} + \int_{x^{1/2}}^{\infty}\frac{\Psi(t,y)}{t^2}\,dt\\ &< 0 + \int_{x^{1/2}}^{\infty}\frac{t^{1/3}}{t^2}\,dt \ll x^{-1/3}\end{aligned}$$

when $x$ is sufficiently large, establishing part (a) of the lemma. Part (b) follows from part (a) upon noting that the number of integers less than $x$ that are divisible by a fixed $y$-friable integer $m > x^{1/2}$ is at most $x/m$ and summing over $m$. □

**Lemma 3.4.** *Let $x \ge 3$, and set $y = 2\log x$. Then*

$$\prod_{p\le y}\Big(1+\frac{1}{p}\Big)^{-1}\sum_{\substack{m\le\sqrt{x}\\ m \text{ is } y\text{-friable}}}\frac{\phi(m)\ell(m)}{m^2} = \Delta + O\Big(\frac{1}{\log x}\Big),$$

*where $\Delta$ is defined in equation* (1.3)*.*

*Proof.* Throughout we may assume that $x$ and hence $y$ are sufficiently large. We first consider the terms in the sum for which the value of $\ell(m)$ is fixed:

$$\sum_{\substack{m\le\sqrt{x}\\ m \text{ is } y\text{-friable}\\ \ell(m)=\ell}}\frac{\phi(m)\ell(m)}{m^2} = \ell\Bigg(\sum_{\substack{m\ge 1\\ m \text{ is } y\text{-friable}\\ \ell(m)=\ell}}\frac{\phi(m)}{m^2} + O\Bigg(\sum_{\substack{m>\sqrt{x}\\ m \text{ is } y\text{-friable}\\ \ell(m)=\ell}}\frac{1}{m}\Bigg)\Bigg). \tag{3.1}$$

The sum inside the error term of equation (3.1), even without the condition $\ell(m)=\ell$, is bounded by a constant times $x^{-1/3}$ by Lemma 3.3(a). On the other hand, the first sum on the right-hand side of (3.1) can be written as the product

$$\begin{aligned}\sum_{\substack{m\ge1\\ m\text{ is }y\text{-friable}\\ \ell(m)=\ell}}\frac{\phi(m)}{m^2}&=\prod_{p<\ell}\bigg(\frac{\phi(p)}{p^2}+\frac{\phi(p^2)}{p^4}+\dots\bigg)\prod_{\ell<p\le y}\bigg(1+\frac{\phi(p)}{p^2}+\frac{\phi(p^2)}{p^4}+\cdots\bigg)\\ &=\bigg(\prod_{p<\ell}\frac1p\bigg)\prod_{\ell<p\le y}\bigg(1+\frac1p\bigg).\end{aligned}$$

Using this information and summing equation (3.1) over the possible values of $\ell(m)$, we conclude that

$$\begin{aligned}\prod_{p\le y}\bigg(1+\frac1p\bigg)^{-1}&\sum_{\substack{m\le\sqrt{x}\\ m\text{ is }y\text{-friable}}}\frac{\phi(m)\ell(m)}{m^2}\\ &=\prod_{p\le y}\bigg(1+\frac1p\bigg)^{-1}\sum_{\ell\le y}\ell\bigg(\bigg(\prod_{p<\ell}\frac1p\bigg)\prod_{\ell<p\le y}\bigg(1+\frac1p\bigg)+O(x^{-1/3})\bigg)\\ &=\sum_{\ell\le y}\frac{\ell^2}{\prod_{p\le\ell}(p+1)}+O(x^{-1/3}y^2)\\ &=\Delta+O\bigg(x^{-1/4}+\sum_{\ell>y}\frac{\ell^2}{\prod_{p\le\ell}(p+1)}\bigg).\end{aligned}$$

It suffices to show that the sum in this error term is $O(1/\log x)$.

When $x$ is sufficiently large, each summand in the error term is less than half the previous summand. (Specifically, this is the case when $y>7$; here we use Bertrand's postulate to bound the ratio between consecutive primes by 2.) Consequently, that sum is bounded above by a geometric series that sums to twice the first term: if $r$ is the smallest prime exceeding $y$ (so that $r\le 2y$), then

$$\sum_{\ell>y}\frac{\ell^2}{\prod_{p\le\ell}(p+1)}<2\frac{r^2}{\prod_{p\le r}(p+1)}<8y^2\exp\bigg(-\sum_{p\le y}\log p\bigg)\ll y^2e^{-c_5y}$$

for some positive constant $c_5$, by Chebyshev's lower bound $\sum_{p\le y}\log p\gg y$. Since $y^3e^{-c_5y}$ is a bounded function for $y\ge1$, we see that $y^2e^{-c_5y}\ll 1/y\ll 1/\log x$, which completes the proof of the lemma. □

We now collect the previous three lemmas together to assist in our evaluation of the main sum appearing in Corollary 1.2.

**Proposition 3.5.** *Let* $\Delta$ *be defined as in equation* (1.3). *Then for* $x\ge3$*,*

$$\sum_{q\le x}\phi(q)\ell(q)=\frac{3\Delta x^2}{\pi^2}+O\bigg(\frac{x^2}{\log x}\bigg)$$

*Proof.* As usual we may assume that $x$ is sufficiently large. We evaluate the sum by sorting the integers $q$ according to their divisors consisting only of small primes. Set $y=2\log x$, and define $Q=\prod_{p\le y}p$. Let $M(q)$ denote the largest $y$-friable divisor of $q$; notice that $\ell(q)=\ell(M(q))$, since $\ell(q)<y$ for all $q\le x$ (when $x$ is sufficiently large).

For a fixed $y$-friable number $m$, the statement $M(q)=m$ is equivalent to $q$ being of the form $q'm$ with $\gcd(q',Q)=1$; note that in this case $\gcd(q',m)=1$ as well, and so

$\phi(q)=\phi(q')\phi(m)$. Consequently, by Lemma 3.2,

$$\begin{aligned}\sum_{\substack{q\le x\\ M(q)=m}} \phi(q)\ell(q) &= \phi(m)\ell(m) \sum_{\substack{q'\le x/m\\ \gcd(q',Q)=1}} \phi(q') \\ &= \phi(m)\ell(m)\frac{3(x/m)^2}{\pi^2}\prod_{p\le y}\biggl(1+\frac{1}{p}\biggr)^{-1} + O\biggl(\phi(m)\ell(m)2^{\pi(y)}\frac{x}{m}\log\frac{x}{m}\biggr).\end{aligned}$$

In the error term, note that $\phi(m)/m\le 1$ and $\ell(m)\log(x/m)\ll \log^2 x$, and also that $2^{\pi(y)}\log^2 x \ll \exp\bigl(O((\log x)/\log\log x)\bigr) \ll x^{1/3}$, say. We thus have

$$\sum_{\substack{q\le x\\ M(q)=m}} \phi(q)\ell(q) = \frac{3x^2}{\pi^2}\frac{\phi(m)\ell(m)}{m^2}\prod_{p\le y}\biggl(1+\frac{1}{p}\biggr)^{-1} + O(x^{4/3}).$$

Summing over $m$, we conclude that

$$\begin{aligned}\sum_{q\le x}\phi(q)\ell(q) &= \sum_{\substack{m\le x\\ m \text{ is } y\text{-friable}}}\ \sum_{\substack{q\le x\\ M(q)=m}} \phi(q)\ell(q) \\ &= \sum_{\substack{m\le \sqrt{x}\\ m \text{ is } y\text{-friable}}} \biggl(\frac{3x^2}{\pi^2}\frac{\phi(m)\ell(m)}{m^2}\prod_{p\le y}\biggl(1+\frac{1}{p}\biggr)^{-1} + O(x^{4/3})\biggr) \\ &\qquad + O\biggl(\sum_{\substack{\sqrt{x}<m\le x\\ m \text{ is } y\text{-friable}}} \phi(m)\ell(m)\biggr).\end{aligned}$$

In this last error term, each summand is at most $xy \ll x^{7/6}$, and the number of summands is $\ll x^{2/3}$ by Lemma 3.3(b). Therefore this equation becomes

$$\sum_{q\le x}\phi(q)\ell(q) = \frac{3x^2}{\pi^2}\prod_{p\le y}\biggl(1+\frac{1}{p}\biggr)^{-1} \sum_{\substack{m\le \sqrt{x}\\ m \text{ is } y\text{-friable}}} \frac{\phi(m)\ell(m)}{m^2} + O(x^{11/6}),$$

which by Lemma 3.4 becomes $\sum_{q\le x}\phi(q)\ell(q) = 3\Delta x^2/\pi^2 + O\bigl(x^2/\log x\bigr)$ as claimed. □

*Proof of Corollary 1.2.* We prove the corollary in the quantitative form

$$\biggl(\sum_{q\le x}\sum_{\substack{\chi \pmod q\\ \chi\ne\chi_0}} 1\biggr)^{-1}\biggl(\sum_{q\le x}\sum_{\substack{\chi \pmod q\\ \chi\ne\chi_0}} n_\chi\biggr) = \Delta + O\biggl(\frac{(\log\log x)^2}{\log x}\biggr).$$

Since the first double sum is well-known to equal

$$\sum_{q\le x}\sum_{\substack{\chi \pmod q\\ \chi\ne\chi_0}} 1 = \sum_{q\le x}(\phi(q)-1) = \frac{3x^2}{\pi^2} + O(x\log x)$$

(the latter equality follows from Lemma 3.2 with $m=1$), it suffices to show that

$$\sum_{q\le x}\sum_{\substack{\chi \pmod q\\ \chi\ne\chi_0}} n_\chi = \frac{3\Delta x^2}{\pi^2} + O\biggl(\frac{x^2(\log\log x)^2}{\log x}\biggr). \tag{3.2}$$

By Theorem 1.1,

$$\sum_{q\le x}\sum_{\substack{\chi \pmod q\\ \chi\ne\chi_0}} n_\chi = \sum_{3\le q\le x}(\phi(q)-1)\biggl(\ell(q)+O\biggl(\frac{(\log\log q)^2}{\log q}\biggr)\biggr)$$
$$= \sum_{3\le q\le x}\phi(q)\ell(q)+O\biggl(\sum_{3\le q\le x}\biggl(\ell(q)+\phi(q)\frac{(\log\log q)^2}{\log q}\biggr)\biggr).$$

We note that $\ell(q)\ll\log x$ uniformly for $q\le x$. Since the function $(\log\log t)^2/\log t$ is bounded for $t\ge 3$ and decreasing for $t>e^{e^2}$, it follows that the error term (for $x$ sufficiently large) is

$$\ll\sum_{q\le x}\log x+\sum_{q\le\sqrt{x}}q+\sum_{\sqrt{x}<q\le x}q\frac{(\log\log\sqrt{x})^2}{\log\sqrt{x}},$$

and so

$$\sum_{q\le x}\sum_{\substack{\chi \pmod q\\ \chi\ne\chi_0}} n_\chi = \sum_{q\le x}\phi(q)\ell(q)+O\biggl(\frac{x^2(\log\log x)^2}{\log x}\biggr).$$

Since $\sum_{q\le x}\phi(q)\ell(q)=3\Delta x^2/\pi^2+O\bigl(x^2/\log x\bigr)$ by Proposition 3.5, this equation establishes the formula (3.2) and hence the corollary. □

It is worth remarking that our methods can address the average value of $n_\chi$, not just over all nonprincipal characters $\chi$, but also over only certain characters. Let $q\ge 3$, and let $\mathscr{X}(q)$ be a nonempty collection of nonprincipal Dirichlet characters modulo $q$. The set of $\chi\in\mathscr{X}(q)$ with $n_\chi>\ell(q)$ is obviously a subset of the set of all nonprincipal $\chi \pmod q$ with $n_\chi>\ell(q)$. This triviality, taken together with the estimates occurring in the proof of Theorem 1.1 and earlier in Section 2, shows that

$$\bigl(\#\mathscr{X}(q)\bigr)^{-1}\sum_{\chi\in\mathscr{X}(q)} n_\chi = \ell(q)+O\biggl(\frac{\phi(q)}{\#\mathscr{X}(q)}\frac{(\log\log q)^2}{\log q}\biggr). \tag{3.3}$$

To take an example of special interest, let $\mathscr{X}(q)$ be the set of primitive characters modulo $q$, and let $\phi^*(q)=\#\mathscr{X}(q)$. From Möbius inversion applied to the relation $\sum_{d\mid q}\phi^*(d)=\phi(q)$, we find that

$$\phi^*(q)=q\prod_{p\parallel q}\biggl(1-\frac{2}{p}\biggr)\prod_{p^2\mid q}\biggl(1-\frac{1}{p}\biggr)^2.$$

Hence, $\phi^*(q)>0$ precisely when $q\not\equiv 2 \pmod 4$, and whenever $\phi^*(q)$ is nonvanishing, we have

$$\phi^*(q)\gg\phi(q)\prod_{p\mid q}\biggl(1-\frac{1}{p}\biggr)\gg\frac{\phi(q)}{\log\log q}.$$

So when $q\not\equiv 2 \pmod 4$, the estimate (3.3) shows that the average of $n_\chi$ taken over primitive characters $\chi$ modulo $q$ is

$$\frac{1}{\phi^*(q)}\sum_{\substack{\chi \pmod q\\ \chi \text{ primitive}}} n_\chi = \ell(q)+O\biggl(\frac{(\log\log q)^3}{\log q}\biggr), \tag{3.4}$$

which is the analogue of Theorem 1.1 for primitive characters. From this, we can deduce a corollary similar to Corollary 1.2. It is necessary to replace Lemma 3.2 with the estimate

$$\sum_{\substack{n\le x\\ \gcd(n,m)=1}} \phi^*(n) = \frac{18x^2}{\pi^4}\biggl(\prod_{p\mid m}\frac{p^3}{(p+1)(p^2-1)}\biggr) + O(2^{\omega(m)}x\log^2 x) \tag{3.5}$$

uniformly in $m$, which can be proved by an argument similar to the proof of Lemma 3.2. Imitating the proof of Corollary 1.2 but using equations (3.4) and (3.5) as input, we can establish:

**Theorem 3.6.** *Define*

$$\Delta^* = \sum_{\ell}\frac{\ell^4}{(\ell+1)^2(\ell-1)}\prod_{p<\ell}\frac{p^2-p-1}{(p+1)^2(p-1)} \approx 2.1514351057,$$

*where the sum and product are taken over primes $\ell$ and $p$. Then*

$$\lim_{x\to\infty}\biggl(\sum_{q\le x}\sum_{\substack{\chi \pmod q\\ \chi\ primitive}} 1\biggr)^{-1}\biggl(\sum_{q\le x}\sum_{\substack{\chi \pmod q\\ \chi\ primitive}} n_\chi\biggr) = \Delta^*.$$

## 4. The least non-split prime averaged over cubic number fields

In this section, we consider cubic extensions $K$ of $\mathbb{Q}$ and investigate the distribution of the least rational prime with a particular factorization into prime ideas in the ring of integers $O_K$. This investigation is most successful in the case of the least prime that does not split completely, where we will be able to establish Theorem 1.3. In other cases (the least completely split prime, the least partially split prime, and the least inert prime), we will be able to establish the analogous Theorem 4.8, but only under the assumption of a generalized Riemann hypothesis.

The first ingredient of the proof of Theorem 1.3 is a now classical theorem of Davenport and Heilbronn [DH71]:

**Proposition 4.1.** *As $x\to\infty$, the number of cubic fields $K$ with $|D_K|\le x$ is $\sim \dfrac{x}{3\zeta(3)}$.*

A refined version of the Davenport–Heilbronn theorem was proposed by Roberts [Rob01] and recently confirmed by Taniguchi and Thorne [TT11] (see also the independent work of Bhargava, Shankar, and Tsimerman [BST10]). One consequence of their work (see [TT11, Theorem 1.3 and Section 6.2]) is the following explicit estimate:

**Proposition 4.2.** *Let $x\ge 1$, and let $1\le y\le \frac{1}{40}\log x$. For each prime $p\le y$, we define local factors $t(p)$ and $t'(p)$, depending on the desired factorization of $p$, as follows:*

$$t(p) = \begin{cases} 1/6 & \text{if } p \text{ is to split completely,}\\ 1/2 & \text{if } p \text{ is to partially split,}\\ 1/3 & \text{if } p \text{ is to be inert,}\\ 1/p & \text{if } p \text{ is to partially ramify,}\\ 1/p^2 & \text{if } p \text{ is to ramify completely,}\end{cases}$$

*and*

$$t'(p) = \frac{t_p}{1+1/p+1/p^2}.$$

*The number of cubic number fields $K$ (up to isomorphism) with $|D_K| \le x$ in which the primes $p \le y$ factor in the specified ways is*

$$\frac{x}{3\zeta(3)} \prod_{p \le y} t'(p) + O(x^{5/6}),$$

*uniformly in the choice of splitting conditions.*

If $K$ is a non-Galois cubic field, then the normal closure of $K/\mathbb{Q}$ contains a unique quadratic subfield, called the *quadratic resolvent* of $K$. If $K$ is cyclic, we adopt the convention that $K$ has quadratic resolvent $\mathbb{Q}$; in both cases, the quadratic resolvent is $\mathbb{Q}(\sqrt{D_K})$. The next lemma provides an upper bound on the number of cubic fields with a given quadratic resolvent. It should be noted that Cohen and Morra [CM11] have asymptotic results for this problem for a *fixed* quadratic resolvent, but in our application we require some uniformity.

**Lemma 4.3.** *Let $L$ be either $\mathbb{Q}$ or a quadratic extension of $\mathbb{Q}$. For $x \ge 1$, the number of cubic fields whose discriminant is at most $x$ in absolute value, and whose quadratic resolvent equals $L$, is $\ll x^{0.84}$ uniformly in $L$.*

*Proof.* Suppose that $K$ has quadratic resolvent $L$ and that $|D_K| \le x$. Then $D_K = f^2 D_L$ for some positive integer $f$ (see for example [Coh93, §6.4.5]). Clearly $f \le x^{1/2}$, and thus the number of choices for $D_K$ is also at most $x^{1/2}$. Ellenberg and Venkatesh [EV07] have shown that the number of cubic fields with discriminant $D$ is $\ll_\epsilon |D|^{1/3+\epsilon}$, and so the lemma follows upon taking $\epsilon = \frac{1}{150}$ and summing over the $x^{1/2}$ possibilities for $D = D_K$. □

**Remark.** The proof actually gives an upper bound of $\ll_\epsilon x^{5/6+\epsilon}/|D_L|^{1/2}$ for the number of such cubic fields, although we will not need this stronger statement.

Recall now that $n_K$ denote the least rational prime that does not split completely in $K$; we are interested in the average value of $n_K$ as $K$ ranges over all cubic fields, ordered by the absolute value of their conductor. To help us handle the contribution to the average from fields $K$ for which $n_K$ is large, we quote two results from the literature. The first, a universal upper bound on $n_K$, is due to Li [Li11]:

**Proposition 4.4.** *If $K$ is a cubic field, then the least non-split prime in $K$ is $\ll |D_K|^{1/7.39}$.*

As discussed by Li, it is much simpler to prove Proposition 4.4 with the larger exponent $1/4\sqrt{e} + \epsilon$, which would also suffice for our purposes.

The next result, in slightly stronger form, appears without proof in a paper of Duke and Kowalski [DK00] (for details, see the proof of [Pol11, Lemma 5.3]). Baier [Bai06] has a sharper result allowing one to replace $2/A$ below with $1/(A-1)$, but we will not need this improvement.

**Proposition 4.5.** *Fix $A > 2$ and $\epsilon > 0$. For any $x \ge 1$, the number of primitive Dirichlet characters $\chi$ of conductor at most $x$ with the property that $\chi(p) = 1$ for all primes $p \le (\log x)^A$ is $\ll_{A,\epsilon} x^{2/A+\epsilon}$.*

This proposition quickly implies a lemma about the scarcity of *quadratic* fields with no small non-split primes.

**Lemma 4.6.** *The number of quadratic fields whose discriminant is at most $x$ in absolute value, in which every prime $p \le (\log x)^{200}$ splits, is $\ll x^{1/99}$.*

*Proof.* There is a bijection between quadratic fields and primitive quadratic characters given by matching the quadratic field of discriminant $D$ with the primitive character $\big(\frac{D}{\cdot}\big)$ of conductor $|D|$ (see for example [MV07, Theorem 9.13, p. 297]). If $L$ is a quadratic field with the properties in the statement of the lemma, then $\chi(\cdot) = \big(\frac{D_L}{\cdot}\big)$ is a primitive character of conductor $|D_L| \le x$ with $\chi(p) = 1$ for all $p \le (\log x)^{200}$. By Proposition 4.5 with $\epsilon = \frac{1}{9900}$, the number of such characters is $\ll x^{1/99}$. □

These preliminary field-counting results enable us to bound an error term that arises in the proof of Theorem 1.3.

**Lemma 4.7.** *Let $x \ge 3$, and let $y = \frac{1}{40}\log x$ and $z = (\log x)^{200}$. There exists an absolute positive constant $c_6$ such that*

$$z \sum_{\substack{|D_K|\le x \\ y<n_K}} 1 + x^{1/7.39} \sum_{\substack{|D_K|\le x \\ z<n_K}} 1 \ll x \exp\left(-\frac{c_6 \log x}{\log\log x}\right),$$

*where the sums range over cubic fields $K$.*

*Proof.* The number of cubic fields $K$ with $|D_K| \le x$ in which every prime $p \le y$ splits completely can be estimated by Proposition 4.2, where we take $t_p = \frac{1}{6}$ for every $p \le y$. In particular, each such $t_p' < \frac{1}{6}$, and so the first term can be bounded by

$$z \sum_{\substack{|D_K|\le x \\ y<n_K}} 1 \ll z\bigg(\frac{x}{6^{\pi(y)}} + x^{5/6}\bigg) \ll (\log x)^{200}\bigg(\frac{x}{\exp(\log 6 \cdot \frac{1}{2}y/\log y)} + x^{5/6}\bigg)$$

$$\ll x \exp\left(-\frac{c_6 \log x}{\log\log x}\right) \tag{4.1}$$

for some positive constant ($c_6 = 0.02$ is valid); we used in the middle estimate a crude Chebyshev-type lower bound for $\pi(y)$.

On the other hand, if $n_K > z$, then either $K$ is already a Galois extension (in which case its quadratic resolvent equals $\mathbb{Q}$) or else every prime $p \le z$ splits completely in the normal closure of $K$, and so also splits in the quadratic resolvent $L$ of $K$ (see [Mar77, Corollary, p. 106]). Lemma 4.6 tells us that the number of such fields $L$ is $\ll x^{1/99}$; for each such $L$, the number of cubic fields $K$ whose quadratic resolvent equals $L$ is $\ll x^{0.84}$ by Lemma 4.3. Therefore the second term can be bounded by

$$x^{1/7.39} \sum_{\substack{|D_K|\le x \\ z<n_K}} 1 \ll x^{1/7.39} x^{1/99+0.84} \ll x^{0.99},$$

which is small enough to establish the desired estimate. □

With Proposition 4.2 still available to handle the smaller values of $n_K$, we are now ready to evaluate the average value of $n_K$ over cubic fields $K$.

*Proof of Theorem 1.3.* We prove the theorem in the quantitative form

$$\bigg(\sum_{|D_K|\le x} 1\bigg)^{-1}\bigg(\sum_{|D_K|\le x} n_K\bigg) = \Delta_{nsc} + O\bigg(\exp\left(-\frac{c_6 \log x}{\log\log x}\right)\bigg),$$

where the sums are taken over cubic fields $K$. Taking $y = 1$ in Proposition 4.2, we deduce a quantitative version of the Davenport–Heilbronn Theorem (Proposition 4.1), namely that the first sum is $x/3\zeta(3) + O(x^{5/6})$. Therefore it suffices to show that

$$\sum_{|D_K|\le x} n_K = \frac{x}{3\zeta(3)}\Delta_{nsc} + O\bigg(x\exp\bigg(-\frac{c_6\log x}{\log\log x}\bigg)\bigg). \tag{4.2}$$

Set $y = \frac{1}{40}\log x$ and $z = (\log x)^{200}$, and write

$$\begin{aligned}\sum_{|D_K|\le x} n_K &= \sum_{\substack{|D_K|\le x\\ n_K\le y}} n_K + \sum_{\substack{|D_K|\le x\\ y<n_K\le z}} n_K + \sum_{\substack{|D_K|\le x\\ z<n_K}} n_K \\ &= \sum_{\ell\le y}\ell \sum_{\substack{|D_K|\le x\\ n_K=\ell}} 1 + O\bigg(z\sum_{\substack{|D_K|\le x\\ y<n_K}} 1 + x^{1/7.39}\sum_{\substack{|D_K|\le x\\ z<n_K}} 1\bigg);\end{aligned} \tag{4.3}$$

in the last sum we have used the universal upper bound for $n_K$ from Proposition 4.4. By Lemma 4.7, this estimate becomes

$$\sum_{|D_K|\le x} n_K = \sum_{\ell\le y}\ell \sum_{\substack{|D_K|\le x\\ n_K=\ell}} 1 + O\bigg(x\exp\bigg(-\frac{c_6\log x}{\log\log x}\bigg)\bigg). \tag{4.4}$$

For any prime $\ell$, the cubic fields $K$ such that $n_K = \ell$ are exactly those fields in which $p$ splits completely for all $p < \ell$, yet $\ell$ does not split completely. Proposition 4.2, summed over the four other possibilities for the factorization of $\ell$, tells us that the number of such fields with $|D_K| \le x$ is

$$\frac{x}{\zeta(3)}\frac{(5/6 + 1/\ell + 1/\ell^2)}{1 + 1/\ell + 1/\ell^2}\prod_{p<\ell}\frac{1/6}{1 + 1/p + 1/p^2} + O(x^{5/6}),$$

and therefore

$$\begin{aligned}\sum_{\ell\le y}\ell \sum_{\substack{|D_K|\le x\\ n_K=\ell}} 1 &= \frac{x}{3\zeta(3)}\sum_{\ell\le y}\frac{\ell(5/6 + 1/\ell + 1/\ell^2)}{1 + 1/\ell + 1/\ell^2}\prod_{p<\ell}\frac{1/6}{1 + 1/p + 1/p^2} + O(y^2x^{5/6}) \\ &= \frac{x}{3\zeta(3)}\Delta_{nsc} + O\bigg(x\sum_{\ell>y}\Big(\ell\prod_{p<\ell}\tfrac{1}{6}\Big) + x^{5/6}\log^2 x\bigg)\end{aligned}$$

by the definition (1.4) of $\Delta_{nsc}$. In this remaining sum, each summand is at most $\frac{1}{3}$ of the previous one by Bertrand's postulate, and so the sum is bounded (up to a multiplicative constant) by the first term; we conclude that

$$\begin{aligned}\sum_{\ell\le y}\ell \sum_{\substack{|D_K|\le x\\ n_K=\ell}} 1 &= \frac{x}{3\zeta(3)}\Delta_{nsc} + O(x\cdot 2y\cdot 6^{-\pi(y)} + x^{5/6}\log x) \\ &= \frac{x}{3\zeta(3)}\Delta_{nsc} + O\bigg(x\exp\bigg(-\frac{c_6\log x}{\log\log x}\bigg)\bigg)\end{aligned}$$

just as in the estimate (4.1). Inserting this result into equation (4.4) establishes equation (4.2) and hence the theorem. □

For each natural number $k$ and each prime $p \equiv 1 \pmod k$, let $r_k(p)$ denote the least prime $k$th power residue modulo $p$. Elliott [Ell71] has shown that for each of $k = 2, 3$, and 4, the function $r_k(p)$ possesses a finite mean value. When $k = 3$, Elliott's result gives the average smallest split prime in cubic extensions of prime conductor.

Motivated by Elliott's work, one might wonder if it is possible to obtain the average least split prime, where the average is instead taken over *all* cubic extensions of $\mathbb{Q}$ (ordered by the absolute value of their discriminant as in Theorem 1.3). One could ask the same question for the least partially split prime or the least inert prime. We can establish the following conditional results, where the averages are taken over cubic fields $K$:

**Theorem 4.8.** *Assume the generalized Riemann hypothesis for Dedekind zeta functions. For each prime $p$, define*

$$t'_{cs}(p) = \frac{1/6}{1+1/p+1/p^2}, \quad t'_{inert}(p) = \frac{1/3}{1+1/p+1/p^2}, \quad \text{and } t'_{ps}(p) = \frac{1/2}{1+1/p+1/p^2}.$$

*The average least completely split prime in a cubic field is*

$$\sum_\ell \ell t'_{cs}(\ell) \prod_{p<\ell} (1 - t'_{cs}(p)) = 19.7952216366\dots.$$

*The average least inert prime is*

$$\sum_\ell \ell t'_{inert}(\ell) \prod_{p<\ell} (1 - t'_{inert}(p)) = 8.5447294614\dots.$$

*Finally, if the average is restricted to non-Galois cubic fields, the average least partially split prime is*

$$\sum_\ell \ell t'_{ps}(\ell) \prod_{p<\ell} (1 - t'_{ps}(p)) = 5.3680248421\dots.$$

*Here all sums and products are taken over primes $\ell$ and $p$.*

The proofs mimic that of Theorem 1.3. However, the proofs (in particular the analogues of Lemma 4.7) are simpler in that the parameter $z$ is no longer required: all values of $n_K$ greater than $y$ in equation (4.3) can be treated together. The reason is that under the generalized Riemann hypothesis, the least unramified prime $p$ with a prescribed splitting type is $\ll \log^2 |D_K|$ (see [LO77], [LMO79]); this conditional universal upper bound for the analogues of $n_K$ is small enough to obviate the need for the second splitting at $z$.

It would be interesting to find an unconditional proof for any of the assertions of Theorem 4.8. The obstacle at present is the lack of an unconditional universal upper bound for the analogues of $n_K$ that could take the place of Proposition 4.4. Currently the best known upper bound for the least completely split prime is $|D|^{c_7}$ for a certain unspecified (and potentially large) absolute constant $c_7$ (see [LMO79, Theorem 1.1]), and similarly for the least inert prime or the least partially split prime.

We conclude with a remark that might be illuminating. Each of the constants in Theorem 4.8 has the form $\sum_\ell \ell t(\ell) \prod_{p<\ell} \big(1 - t(\ell)\big)$, where $t(\ell)$ is the "probability" that the desired property holds for the prime $\ell$. This sum is exactly the form the expectation would have if each prime were replaced by a random event $X_\ell$ that took place with probability $t(\ell)$, as long as the events $X_\ell$ were independent. The constant $\Delta_{nsc}$ in Theorem 1.3 also has this form, and in fact so do the constants on the right-hand sides of equations (1.2) and even (1.1) (where $t(p) = \frac{1}{2}$ reflects the fact that each prime is expected to be a quadratic residue exactly half of the time). The calculations of these average-value results demonstrate that these properties of small primes are indeed asymptotically independent; in the aforementioned situations it is quite helpful that the sums converge so rapidly that only the small primes are relevant.

## Acknowledgements

The authors thank Carl Pomerance for helpful conversations and Mits Kobayashi for technical assistance with Karim Belabas's `cubics` package.

## References

[Ank52] N. C. Ankeny, *The least quadratic non residue*, Ann. of Math. (2) **55** (1952), 65–72.

[Bac90] E. Bach, *Explicit bounds for primality testing and related problems*, Math. Comp. **55** (1990), no. 191, 355–380.

[Bai06] S. Baier, *On the least $n$ with $\chi(n) \neq 1$*, Q. J. Math. **57** (2006), no. 3, 279–283.

[Bel97] K. Belabas, *A fast algorithm to compute cubic fields*, Math. Comp. **66** (1997), no. 219, 1213–1237, software package `cubics` available from `http://www.math.u-bordeaux1.fr/∼belabas/research/`.

[Bel04] ———, *On quadratic fields with large 3-rank*, Math. Comp. **73** (2004), no. 248, 2061–2074.

[BH96] R. C. Baker and G. Harman, *The Brun-Titchmarsh theorem on average*, Analytic number theory, Vol. 1 (Allerton Park, IL, 1995), Progr. Math., vol. 138, Birkhäuser Boston, Boston, MA, 1996, pp. 39–103.

[BH98] ———, *Shifted primes without large prime factors*, Acta Arith. **83** (1998), no. 4, 331–361.

[BST10] M. Bhargava, A. Shankar, and J. Tsimerman, *On the Davenport-Heilbronn theorem and second order terms*, e-print at `arXiv:1005.0672 [math.NT]`.

[Bur97] R. J. Burthe, Jr., *The average least witness is* 2, Acta Arith. **80** (1997), no. 4, 327–341.

[CM11] H. Cohen and A. Morra, *Counting cubic extensions with given quadratic resolvent*, J. Algebra **325** (2011), 461–478.

[Coh93] H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics, vol. 138, Springer-Verlag, Berlin, 1993.

[DH71] H. Davenport and H. Heilbronn, *On the density of discriminants of cubic fields. II*, Proc. Roy. Soc. London Ser. A **322** (1971), no. 1551, 405–420.

[DK00] W. Duke and E. Kowalski, *A problem of Linnik for elliptic curves and mean-value estimates for automorphic representations*, Invent. Math. **139** (2000), no. 1, 1–39.

[Ell68] P. D. T. A. Elliott, *A problem of Erdős concerning power residue sums*, Acta Arith. **13** (1967/1968), 131–149.

[Ell71] ———, *The least prime k-th-power residue*, J. London Math. Soc. (2) **3** (1971), 205–210.

[Erd61] P. Erdős, *Remarks on number theory. I*, Mat. Lapok **12** (1961), 10–17 (Hungarian).

[EV07] J. S. Ellenberg and A. Venkatesh, *Reflection principles and bounds for class group torsion*, Int. Math. Res. Not. IMRN (2007), no. 1, Art. ID rnm002, 18 pp.

[Jut77] M. Jutila, *On Linnik's constant*, Math. Scand. **41** (1977), no. 1, 45–62.

[KP05] P. Kurlberg and C. Pomerance, *On the periods of the linear congruential and power generators*, Acta Arith. **119** (2005), no. 2, 149–169.

[Li11] X. Li, *The smallest prime that does not split completely in a number field*, Algebra and Number Theory (2011), to appear, e-print at `arXiv:1003.5718 [math.NT]`.

[LMO79] J. C. Lagarias, H. L. Montgomery, and A. M. Odlyzko, *A bound for the least prime ideal in the Chebotarev density theorem*, Invent. Math. **54** (1979), no. 3, 271–296.

[LO77] J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem*, Algebraic number fields: $L$-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London, 1977, pp. 409–464.

[Mar77] D. A. Marcus, *Number fields*, Universitext, Springer-Verlag, New York, 1977.

[Mon94] H. L. Montgomery, *Ten lectures on the interface between analytic number theory and harmonic analysis*, CBMS Regional Conference Series in Mathematics, vol. 84, Published for the Conference Board of the Mathematical Sciences, Washington, DC, 1994.

[MV07] H. L. Montgomery and R. C. Vaughan, *Multiplicative number theory. I. Classical theory*, Cambridge Studies in Advanced Mathematics, vol. 97, Cambridge University Press, Cambridge, 2007.

[Nor98] K. K. Norton, *A character-sum estimate and applications*, Acta Arith. **85** (1998), no. 1, 51–78.

[Pol11] P. Pollack, *The average least quadratic nonresidue modulo $m$ and other variations on a theme of Erdős*, submitted, available from `http://www.math.ubc.ca/∼pollack/work.html`.

[Rob01] D. P. Roberts, *Density of cubic field discriminants*, Math. Comp. **70** (2001), no. 236, 1699–1705 (electronic).

[Ser73] J.-P. Serre, *A course in arithmetic*, Springer-Verlag, New York, 1973.

[Ten95] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Studies in Advanced Mathematics, vol. 46, Cambridge University Press, Cambridge, 1995.

[TT11] T. Taniguchi and F. Thorne, *Secondary terms in counting functions for cubic fields*, submitted, e-print at `arXiv:1102.2914 [math.NT]`.

University of British Columbia, Department of Mathematics, Room 121, 1984 Mathematics Road, Vancouver, BC Canada V6T 1Z2

*E-mail address*: `gerg@math.ubc.ca`

*E-mail address*: `pollack@math.ubc.ca`